REMARKS

Claims 1-20 are currently in the application.

I. DOUBLE PATENTING REJECTIONS

The Examiner has provisionally rejected claims 1-7, 10-14, and 19-20 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-39 of copending Application No. 09/270,967. The Examiner has also rejected claims 1-3, 6, 10-12, and 19 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-42 of U.S. Patent No. 6,353,614. Terminal disclaimers are being filed herewith to overcome these rejections, and Applicants respectfully request that the Examiner withdraw the double patenting rejections.

II. CLAIM REJECTIONS UNDER 35 U.S.C. §103

Claims 1-20 stand rejected as being unpatentable over Tsuruoka (U.S. Patent No. 6,101,189) in view of Ylonen (U.S. Patent No. 6,438,612). The Applicants traverse the Examiners contention that there is suggestion to combine Tsuruoka and Ylonen. Moreover, the combination of these two references is improper and yields an inoperative combination. The Examiner's rejection under §103 is improper and should therefore be withdrawn.

As an initial matter, it is important to keep in mind that all of the pending claims recite a Security Association ("SA") between an internal network device and an external network device that are connected via a router/gateway. For example, Claim 1 of the present application recites "providing a first network device [internal network device] and a second network device [router/gateway] on a first network" and "establishing a security association [SA] between the first network device [internal network device] and a third network device [external network device] on a second network external to the first network." As known in the art, the SA ensures

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001

that packets are secure between the entire end-to-end path of the communication between the internal and external network devices (i.e., the network devices for which the SA was established). Securing only a portion of the communication path, such as between only the internal network device and the router/gateway, between only the external network device and the router/gateway, or between only a pair of routers/gateways, does not constitute an SA between the internal and external network devices. Consequently, as explained more fully below, neither Tsuruoka nor Ylonen anticipate or render obvious, alone or in combination, the present claims.

The Final Office Action admits that Tsuruoka does not disclose the use of security associations or any form of IP security. In fact, the Final Office Action turns to Ylonen to cure this admitted deficiency. The Final Office Action does not provide, however, a sufficient reference to a motivation, teaching, or suggestion to combine the Network Address Translation ("NAT") of Tsuruoka with the IP security of Ylonen. In order to combine the Tsuruoka and Ylonen references, there must be a clear teaching or suggestion to make the combination. *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999). For a combination of references to be proper, the Office Action must provide a showing of a teaching or motivation to combine the references. *Id.* That "showing must be clear and particular." *Id.* Here, the Final Office Action has provided no showing of any teaching or suggestion to combine the Tsuruoka and Ylonen references, let alone a "clear and particular showing."

Instead, the Final Office Action appears to rely on the alleged knowledge of one of ordinary skill in the art to the make the combination. In this regard, it is improper to simply recite the knowledge of one of ordinary skill in the art. Rejections under §103 must be based on evidence. *In re Lee*, 277 F.3d 1338, 1342-43 (Fed. Cir. 2002). "The factual inquiry whether to

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001

combine references must be thorough and searching," and simply reciting common knowledge is not a substitute for evidence of a teaching, motivation, or suggestion to combine references. *Id.* at 1343. Thus, the combination of Tsuruoka and Ylonen is not proper.

The impropriety of combining Tsuruoka and Ylonen is further evidenced by the fact that such a combination would only yield an inoperative combination. Indeed, an examination of the disclosure of these two references demonstrates that there is actually a teaching against combining the Tsuruoka and Ylonen patents. For example, Tsuruoka teaches NAT through a gateway, which requires converting, modifying, and determining content of packets that pass through the gateway. *See* Tsuruoka, col. 12 lines 59-67; col. 13 lines 3-12 and lines 55-60; col. 14 lines 5-25 and lines 36-40. Specifically, Tsuruoka explicitly requires that certain IP addresses and ports in packets be ***replaced*** at the gateway. In fact, that is how NAT works and routes packets. As explained in Tsuruoka, for a packet being sent from a computer on the local network to a computer on the external network via a NAT gateway:

> . . . the source address of the originated packet is ***replaced*** by the source address (myaddr) for the external network interface provided in the gateway apparatus. The source port number of the packet is ***replaced*** by the external network interface port number (xport) registered in the conversion table (step S17). . . . When the packet header information is properly ***altered***, the packet is transmitted to the external network interface, thus completing the routing operation (step S18).

Tsuruoka, col. 9, lines 32-38, 47-49 (emphasis added); *see also*, Tsuruoka, col. 7, lines 1-28. For a packet being sent from a computer on the external network to a computer on the internal network via the NAT gateway, Tsuruoka further explains:

> The arriving packet is then translated such that the destination port number (DP) is ***replaced*** by the source port number (SP) stored in the table at the matching combination; and the destination address (DA) is ***replaced*** by the source address (SA) stored in the table at the matching combination. . . . The packet having the header thereof ***translated*** is then transmitted to the local network.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001

Tsuruoka, col. 10, lines 20-25, 27-28 (emphasis added); *see also*, Tsuruoka, col. 7, lines 1-10, 29-44.

Tsuruoka does not disclose the use of any IP security, and Tsuruoka does not disclose any form of tunneling (either secure or non-secure) between an internal network device and an external network device. In fact, the only method disclosed by Tsuruoka for routing packets between an internal network device and an external network device is via the connecting gateway's use of NAT with the replacing of IP addresses and ports.

In contrast to Tsuruoka, Ylonen teaches a secure communication tunnel established between two virtual routers on two separate virtual networks with IPSEC protocols utilizing IKE SA, or ESP transforms. *See* Ylonen, col. 4 lines 39-67 and col. 5 lines 1-4. Ylonen does not disclose a secure communication channel, however, between an internal network device and an external network device that are connected via a router/gateway. Ylonen also does not disclose, and in fact, teaches away from, any conversion or modification of the packets passing through its two virtual routers/gateways. The reason that Ylonen does not make such a disclosure is abundantly clear – use of IPSEC protocols precludes conversion or modification of packets passing through these virtual routers/gateways.

As known in the art, once an IP packet is protected by IPSEC, it cannot be converted or modified anywhere along its path from the transmitting computer device to the receiving computer device. The background section of the present patent application provides a detailed description of IPSEC and the problems with using NAT together with IPSEC:

> IPSEC currently includes two security services, each having an associated header that is added to an IP packet that is being protected. The two security services include an Authentication Header ("AH") and an Encapsulating Security Payload ("ESP") header. The Authentication Header provides authentication and integrity protection for an IP packet. The Encapsulating Security Payload header provides encryption protection and authentication for an IP packet.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001

The IPSEC protocol headers are identified in a protocol field of an IP data packet header. The IPSEC protocol header specifies the type (e.g., Authentication Header or Encapsulating Security Payload) and contains a numerical value called the Security Parameter Index ("SPI"). The Security Parameter Index together with a destination IP address and Internet Security protocol form a unique identifier used by a receiving system to associate a data packet with a construct called a "security association." The Security Parameter Index is used by the receiving system to help correctly process an IP packet (e.g., to decrypt it, or to verify its integrity and authenticity).

IPSEC establishes and uses a Security Association ("SA") to identify a secure channel between two endpoints. A Security Association is a unidirectional session between two termination endpoints. Two termination endpoints of a single Security Association define a logical session that is protected by IPSEC services. One endpoint sends IP packets, and a second endpoint receives the IP packets. Since a Security Association is unidirectional, a minimum of two Security Associations is required for secure, bi-directional communications. It is also possible to configure multiple layers of IPSEC protocols between two endpoints by combining multiple Security Associations.

There are several problems associated with using current versions of NAT when security is required and the IPSEC protocol is used. Current versions of NAT violate certain specific principles of the IPSEC protocol that allow establishment and maintenance of secure end-to-end connections of an IP network.

A NAT router typically needs to modify an IP packet (e.g., network ports, etc.). However, once an IP packet is protected by IPSEC, it must not be modified anywhere along a path from an IPSEC source to an IPSEC destination. Most NAT routers violate IPSEC by modifying, or attempting to modify individual IP packets.

Even if a NAT router does not modify data packets it forwards, it must be able to read network port numbers (e.g., TCP, UDP, etc.) in the data packets. If certain IPSEC features are used (e.g., Encapsulated Security Payload ("ESP")), the network port numbers are encrypted, so the NAT router typically will not be able to use the network ports for NAT mapping.

Local host network devices on a Local Area Network ("LAN") that use NAT typically possess only local, non-unique IP addresses. The local non-unique IP addresses do not comprise a name space that is suitable for binding an encryption key (e.g., a public key) to a unique entity. Without this unique binding, it is not possible to provide necessary authentication for establishment of Security Associations. Without authentication, an endpoint of a connection cannot be certain of the identity of another endpoint, and thus cannot establish a secure and trusted connection.

Patent Application, p. 5, ln. 19 to p. 7, ln. 15 (emphasis added).

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001

As noted above, Tsuruoka discloses a typical NAT gateway that relies on modification of its data packets wherein IP addresses and ports are replaced. Consequently, the authentication and integrity required for packets in an SA between an internal network device and an external network device, like the SA recited in the present claims, would be destroyed by Tsuruoka's use of NAT. That is, if the NAT gateway of Tsuruoka could even see the IP addresses and/or ports in the packets passing there-through. When packets passing through the gateway are encrypted using IPSEC protocols (e.g., ESP), the NAT gateway of Tsuruoka would not even be able to read the encrypted IP addresses and/or ports of the packets that needed to be replaced, thereby making it impossible for the NAT gateway to properly route received packets.

Accordingly, Tsuruoka used in conjunction with Ylonen renders Tsuruoka inoperable; similarly, Ylonen used in conjunction with Tsuruoka renders Ylonen inoperable, as Tsuruoka requires the modification of IP packets during routing of the packets between the gateway and a computer device, while Ylonen requires that IP packets remain unmodified during transmittal. In effect, Ylonen teaches away from the art taught in Tsuruoka (and vice-versa).

A proposed modification of a prior art reference with another reference is inappropriate when the modification renders the prior art reference inoperable for its intended purpose. *In Re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1894). Moreover, evidence showing there is no reasonable expectation of success supports a conclusion of nonobviousness. *In re Rinehart,* 531 F.2d 1048, 189 USPQ 143 (CCPA 1976). Modifying Tsuruoka with Ylonen, or vice-versa, would render either of the references inoperable for its intended purpose, and have no reasonable expectation of success. Therefore, the combination of these two references is improper and the rejection of the present claims under §103 must be withdrawn.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001

III. SUMMARY

Applicants respectfully submit that, in view of the remarks above, the present application, including claims 1-20, is in condition for allowance, and Applicants solicit action to that end.

If there are any additional matters which may be resolved through a telephone interview, the Examiner is respectfully requested to contact Applicants' undersigned representative.

Respectfully submitted,

McDonnell Boehnen Hulbert & Berghoff LLP

Date: July 20, 2004

By: _____

Sean M. Sullivan
Reg. No. 40,191

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, IL 60606
(312) 913-0001